

jc864 U.S. PTO
09/645588
08/25/00


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

08/25/00
U.S. PTO
Barcode

Applicant: Seigo ARITA
Title: SECURE PARAMETER
GENERATING DEVICE AND
PARAMETER GENERATING
METHOD IN ALGEBRAIC CURVE
CRYPTOGRAPHY

Appl. No.: Unassigned

Filing Date: 08/25/2000

Examiner: Unassigned

Art Unit: Unassigned

UTILITY PATENT APPLICATION
TRANSMITTAL

Assistant Commissioner for Patents
Box PATENT APPLICATION
Washington, D.C. 20231

Sir:

Transmitted herewith for filing under 37 C.F.R. § 1.53(b) is the nonprovisional utility patent application of:

Seigo ARITA

Enclosed are:

- Specification, Claim(s), and Abstract (100 pages).
- Formal drawings (6 sheets, Figures 1-6).
- Declaration and Power of Attorney (2 pages).
- Assignment of the invention to NEC CORPORATION.
- Assignment Recordation Cover Sheet.
- Claim for Convention Priority w/ 1 certified document.
- Information Disclosure Statement.
- Form PTO-1449 with copies of 3 listed reference(s).

The filing fee is calculated below:

Claims as Filed	Included in Basic Fee	Extra Claims	Rate	Fee Totals
Basic Fee			\$690.00	\$690.00
Total Claims: 39	- 20	= 19	x \$18.00	= \$342.00
Independents: 7	- 3	= 4	x \$78.00	= \$312.00
If any Multiple Dependent Claim(s) present:			+ \$260.00	= \$0.00
Assignment Recordation Fee:			+ \$40.00	= \$40.00
			SUBTOTAL:	= \$1384.00
[]	Small Entity Fees Apply (subtract 1/2 of above):			= \$0.00
			TOTAL FILING FEE:	= \$1384.00

[X] A check in the amount of \$1384.00 to cover the filing fee is enclosed.

[] The required filing fees are not enclosed but will be submitted in response to the Notice to File Missing Parts of Application.

[X] The Assistant Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Assistant Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

Please direct all correspondence to the undersigned attorney or agent at the address indicated below.

Respectfully submitted,

Date August 25, 2000

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

By Philip J. Artiola *Reg. No.
38819*
for / David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

SECURE PARAMETER GENERATING DEVICE AND PARAMETER
GENERATING METHOD IN ALGEBRAIC CURVE CRYPTOGRAPHY

BACKGROUNDS OF THE INVENTION

5 FIELD OF THE INVENTION

The present invention relates to a secure parameter generating device, a generating method, and a storing medium in a discrete logarithm cryptography (hereinafter, referred to an algebraic curve 10 cryptography), and more particularly to a secure parameter generating device and its generating method in a discrete logarithm cryptography using Jacobian group of algebraic curve.

15 DESCRIPTION OF THE RELATED ART

A discrete logarithm cryptography is a public key system based on the difficulty of a discrete logarithm problem on a given finite field. In order to keep the security of cryptography, the order of the finite field must be almost a prime number, that is, a 20 factor of small integer and large integer. The algebraic curve cryptography that is one of the discrete logarithm cryptography needs to use an algebraic curve such that the order of the Jacobian group is almost a prime number.

25 In the case of an elliptic curve that is the simplest algebraic curve, an efficient algorithm of calculating the order of the Jacobian group over any elliptic curve is known. The detailed description is

2002-09-26 10:54:50

shown in, for example, "Counting points on elliptic curves over finite fields", Journal de Theorie des Nombres, de Bordeaux 7 (1995), 219-254, Institut de Mathematique de Bordeaux, written by Rene Schoof. The 5 elliptic curve such that the order of the Jacobian group is almost a prime factor can be obtained as follows, by using the above algorithm.

1. Generate a random elliptic curve E .
2. Calculate the order n of the Jacobian group 10 of E .
3. If n is almost a prime number, output E ; otherwise, return to 1.

In the case of an algebraic curve other than an 15 elliptic curve, no efficient algorithm of calculating the order of the Jacobian group is known except for one hyper-elliptic curve. Therefore, the algebraic curve which can be used in the algebraic curve cryptography is limited to an elliptic curve or one exceptional hyper 20 elliptic curve.

As for the h -fold operation of the elements in the Jacobian group, "Software Installation of Discrete Logarithm Cryptography Using C_{ab} curve" written by Arita, Yoshikawa, and Miyauchi, pp.573-578, Security Symposium 25 on Cryptography and Information in 1999, is known.

Further, the technique disclosed in Japanese Patent Publication Laid-Open (Kokai) No. Heisei 6-282226

comprises a step of selecting any prime number, storing
an encryption key corresponding to the prime number into
the public file device, generating a decoding key list
corresponding to the prime number and the encryption key,
5 and storing the decoding key list together with the
prime number into a decoder, wherein an encoder obtains
a public key of a receiver (decoder) from the public
file, to multiply the plaintext on an elliptic curve,
its value is sent to the decoder as a cryptogram, and
10 the decoder computes a parameter of the elliptic curve
from the cryptogram and selects a decoding key
corresponding to the parameter by use of the decoding
key list, thereby obtaining the plaintext from the value
obtained by multiplying the cryptogram by the elliptic
15 curve, using Chinese residue theorem.

The above mentioned conventional technique
limits the usable algebraic curves to an elliptic curve
or one of exceptional hyper-elliptic curve. Since the
elliptic curve and the hyper-elliptic curve are
20 extremely particular algebraic curve from the viewpoint
of the whole algebraic curves and this narrows the
target for cryptanalysis, there arises a security
problem of an algebraic curve cryptography.

25

SUMMARY OF THE INVENTION

An object of the present invention is to make it
possible to use a higher and complicated algebraic curve

which couldn't be used, for an algebraic curve
cryptography, and to provide a secure parameter
generating device in an algebraic curve cryptography for
improving the security of the algebraic curve
cryptography.

Further, another object of the present invention
is to make it possible to use a higher and complicated
algebraic curve which couldn't be used, for an algebraic
curve cryptography, and to provide a secure parameter
generating method in the algebraic cryptography for
improving the security of the algebraic curve
cryptography.

According to the first aspect of the invention,
a secure parameter generating device in an algebraic
curve cryptography, comprises

an input means for receiving two different prime
numbers (a, b) specifying degree of complexity of a
curve and size (n) of an encryption key to be used,

a Stickelberger element computing device for
computing a Stickelberger element (ω) in an ab
cyclotomic, based on the prime number (a) and the prime
number (b),

a Jacobian addition candidate value computing
device for computing Jacobian addition candidate value j
corresponding to the two different prime numbers a and b,
and a prime number p corresponding to the Jacobian
addition candidate value j , based on the prime number

EPO EPO EPO EPO EPO EPO EPO EPO EPO

(a), the prime number (b), the size (n) of an encryption key, and the Stickelberger element (ω) ,

an order candidate value computing device for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b, based on the prime number a, the prime number b, and the Jacobian addition candidate value j,

a security judging device for searching for a candidate value h meeting a security condition such as almost prime number characteristic from the class H , according to the class H ,

a parameter deciding device for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a , the prime number b , and the prime number p , based on the prime number a , the prime number b , the prime number p , and the candidate value h , and

an output device for supplying the parameter of the algebraic curve computed by said parameter deciding device.

In the preferred construction, a secure parameter generating device in an algebraic curve cryptography further comprises

an a-storing means, a b-storing means, and an n-storing means for respectively storing the prime number

a, the prime number b, and the size n of the encryption key received by said input means,

5 a ω -storing means for storing a Stickelberger element ω computed by said Stickelberger element computing device,

a p-storing means and a j-storing means for respectively storing the prime number p and the Jacobian addition candidate value j computed by said Jacobian addition candidate value computing device,

10 an H-storing means for storing the class H computed by said order candidate value computing device, and

an h-storing means for storing the candidate value h found by said security judging device.

15 In another preferred construction, a secure parameter generating device in an algebraic curve cryptography comprises

20 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b.

In another preferred construction, a secure parameter generating device in an algebraic curve cryptography comprises

5 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$.

15 In another preferred construction, a secure parameter generating device in an algebraic curve cryptography comprises

20 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic 25 (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b , and

25 said Jacobian addition candidate value computing

STICKELBERGER ELEMENT COMPUTING DEVICE

device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length
5 $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$.

10 In another preferred construction, a secure parameter generating device in an algebraic curve cryptography comprises

15 said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1,
20 based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

25 In another preferred construction, a secure parameter generating device in an algebraic curve cryptography comprises

said Stickelberger element computing device for computing the Stickelberger element ω by use of the

equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b, and

5 said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

10 In another preferred construction, a secure parameter generating device in an algebraic curve 15 cryptography comprises

20 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 25 $2n/(a-1)(b-1)$ or so, based on the prime number a, the

OPEN SOURCE LICENSE

prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$, and

5 said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

10 In another preferred construction, secure parameter generating device in an algebraic curve cryptography comprises

15 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b ,

5 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the

10 equation $j = \gamma^\omega$, and

15 said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the

20 class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

 In another preferred construction, a secure parameter generating device in an algebraic curve cryptography comprises

25 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a , the prime number b , the prime number

p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^1 Y^a + \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, 5 computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^1 , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number 10 a and the prime number b if the result is equal to an identity element in the Jacobian group.

In another preferred construction, a secure parameter generating device in an algebraic curve 15 cryptography comprises

15 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not 20 exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b, and

25 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on

the prime number a , the prime number b , the prime number p , and the candidate value h , generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^{-m} x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, 5 computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^{-1} , and ζ_b^{-m} as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value 10 h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

In another preferred construction, a secure 15 parameter generating device in an algebraic curve cryptography comprises

said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose 20 absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the 25 equation $j = \gamma^\omega$, and

said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1

with the prime number p used as the divisor, based on the prime number a , the prime number b , the prime number p , and the candidate value h , generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} Y_a + \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of 10 the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

15 In another preferred construction, a secure parameter generating device in an algebraic curve cryptography comprises

said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the 20 parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the 25 class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$, and said parameter deciding device for requiring the

PENDING PUBLICATION

primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point 5 G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^{-m} x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^{-m} 10 as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

15 In another preferred construction, a secure parameter generating device in an algebraic curve cryptography comprises

20 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t 25 indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b,

5 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$, and

10

15 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a , the prime number b , the prime number p , and the candidate value h , generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

20

25

In another preferred construction, a secure parameter generating device in an algebraic curve

cryptography comprises

5 said Stickelberger element computing device for
computing the Stickelberger element ω by use of the
equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs
on a typical series of irreducible residue class with ab
used as a divisor, $[\lambda]$ indicates the maximum integer not
exceeding a rational number λ , $\langle \lambda \rangle$ indicates a
fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t
indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic
10 (ζ is the primitive ab root of 1)), based on the prime
number a and the prime number b,

15 said order candidate value computing device for
computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab
cyclotomic K), as for each k that is an integer from 1
to $2ab$ inclusively, when ζ is the primitive ab root of 1,
based on the prime number a, the prime number b, and the
20 Jacobian addition candidate value j, and computing the
class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$, and

25 said parameter deciding device for requiring the
primitive a root ζ_a and the primitive b root ζ_b of 1
with the prime number p used as the divisor, based on
the prime number a, the prime number b, the prime number
p, and the candidate value h, generating a random point
G over an algebraic curve defined by the equation $\zeta_a^{-1} Y^a$

+ $\zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

10 In another preferred construction, a secure
parameter generating device in an algebraic curve
cryptography comprises

15 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the
20 Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$,

25 said order candidate value computing device for
computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab

5 cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \dots, h_{2ab}\}$, and

10 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^{-m} x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group 15 indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^{-m} as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an 20 identity element in the Jacobian group.

In another preferred construction, a secure parameter generating device in an algebraic curve cryptography comprises

25 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab

used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle\lambda\rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (5 ζ is the primitive ab root of 1)), based on the prime number a and the prime number b,

10 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω , and computing the 15 Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$,

20 said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the 25 Jacobian addition candidate value j, and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$, and said parameter deciding device for requiring the

OPENED SOURCE DOCUMENT

primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} Y^a + \zeta_b^{-m} X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^{-m} as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

According to the second aspect of the invention, a secure parameter generating method in an algebraic curve, comprises the steps of

a Stickelberger element computing procedure for computing a Stickelberger element ω in an ab cyclotomic, respectively based on two different prime numbers a and b specifying degree of complexity of curve,

a Jacobian addition candidate value computing procedure for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b, and a prime number p corresponding to the Jacobian addition candidate value j, respectively based on the prime number a, the prime number b, the size n of

an encryption key, and the Stickelberger element ω ,

an order candidate value computing procedure for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b , respectively based on the prime number a , the prime number b , and the Jacobian addition candidate value j ,

a security judging procedure for searching for a candidate value h meeting a security condition such as almost prime number characteristic from the class H , according to the class H , and

a parameter deciding procedure for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a , the prime number b , and the prime number p , respectively based on the prime number a , the prime number b , the prime number p , and the candidate value h .

In the preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

a procedure for storing a Stickelberger element ω computed by said Stickelberger element computing procedure into said ω -storing means,

a procedure for respectively storing the prime number p and the Jacobian addition candidate value j

OPENED: 2023-01-12 10:00:00

computed by said Jacobian addition candidate value computing procedure into said p-storing means and j-storing means,

5 a procedure for storing the class H computed by said order candidate value computing procedure into said H-storing means, and

a procedure for storing the candidate value h found by said security judging procedure into said h-storing means.

10 In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

15 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b.

20

25 In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

said Jacobian addition candidate value computing procedure for generating α at random, which is an

PUBLISHED BY THE GOVERNMENT OF CANADA 1990

algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a ,
5 the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$.

In another preferred construction, a secure
10 parameter generating method in an algebraic curve cryptography comprises

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b , and

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a ,

DISCLOSED PURSUANT TO 5 U.S.C. § 1417

the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$.

5 In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

10 said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

15 In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

20 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t

DRAFT - 10/10/2013

indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b, and

5 said order candidate value computing procedure
for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1
10 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

15 In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

20 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the
25 equation $j = \gamma^\omega$, and

26 said order candidate value computing procedure

OPEN SOURCE LICENSE

for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

10 In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

15 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b ,

20 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit

length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$, and

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

20 said parameter deciding procedure for requiring
 the primitive a root ζ_a and the primitive b root ζ_b of 1
 with the prime number p used as the divisor, based on
 the prime number a, the prime number b, the prime number
 p, and the candidate value h, generating a random point
 G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a$
 25 $+ \zeta_b^{-m} x^b + 1 = 0$, as for each integer l from 1 to a
 inclusively and each integer m from 1 to b inclusively,
 computing the h-fold of an element in the Jacobian group

indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an 5 identity element in the Jacobian group.

In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

10 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime 15 number a and the prime number b, and

20 said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point 25 G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively,

computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^1 , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value 5 h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

In another preferred construction, a secure parameter generating method in an algebraic curve 10 cryptography comprises

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit 15 length $2n/(a-1)(b-1)$ or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation j = γ^ω , and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point 25 G over an algebraic curve defined by the equation $\zeta_a^1 y^a + \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a

PENDING PUBLICATION

inclusively and each integer m from 1 to b inclusively, computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of
5 the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

In another preferred construction, a secure
10 parameter generating method in an algebraic curve
cryptography comprises

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the
15 parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the
20 Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$, and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on
25 the prime number a , the prime number b , the prime number p , and the candidate value h , generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a$

+ $\zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

10 In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

15 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b,

20 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit

SECURED BY GOVERNMENT CONTRACT

length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$, and

5 equation $j = \gamma^\omega$, and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

25 said Stickelberger element computing procedure
for computing the Stickelberger element ω by use of the
equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (where, t runs
on a typical series of irreducible residue class with ab

used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle\lambda\rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b,

5 said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the 10 parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the 15 Jacobian addition candidate value j, and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$, and

20 said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^{-m} x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, 25 computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^{-m} as the parameter of an algebraic curve whose order of

OPENED: 02/20/2018 09:45:20

the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

5 In another preferred construction, a secure parameter generating method in an algebraic curve cryptography comprises

10 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$,

15 said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$, and

DRAFT PENDING EXAMINER'S REVIEW

5 said parameter deciding procedure for requiring
the primitive a root ζ_a and the primitive b root ζ_b of 1
with the prime number p used as the divisor, based on
the prime number a, the prime number b, the prime number
p, and the candidate value h, generating a random point
G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a$
+ $\zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a
inclusively and each integer m from 1 to b inclusively,
computing the h-fold of an element in the Jacobian group
10 indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m
as the parameter of an algebraic curve whose order of
the Jacobian group is in accord with the candidate value
h, of the algebraic curves specified by the prime number
a and the prime number b if the result is equal to an
15 identity element in the Jacobian group.

In another preferred construction, a secure
parameter generating method in an algebraic curve
cryptography comprises

20 said Stickelberger element computing procedure
for computing the Stickelberger element ω by use of the
equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (where, t runs
on a typical series of irreducible residue class with ab
used as a divisor, $[\lambda]$ indicates the maximum integer not
exceeding a rational number λ , $\langle \lambda \rangle$ indicates a
25 fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t
indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic
(ζ is the primitive ab root of 1)), based on the prime

PENDING PUBLICATION

number a and the prime number b,

5 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω , and computing the
10 Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$,

15 said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the
20 Jacobian addition candidate value j, and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$, and

25 said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a$

+ $\zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^1 , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

10 According to another aspect of the invention, a computer readable memory storing a program for generating a secure parameter in an algebraic curve cryptography, to run the program on a computer,

the program comprises the steps of

15 a Stickelberger element computing procedure for computing a Stickelberger element ω in an ab cyclotomic, respectively based on two different prime numbers a and b specifying degree of complexity of curve,

20 a Jacobian addition candidate value computing procedure for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b, and a prime number p corresponding to the Jacobian addition candidate value j, respectively based on the prime number a, the prime number b, the size n of an encryption key, and the Stickelberger element ω ,

25 an order candidate value computing procedure for computing a class H consisting of a plurality of

candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b, respectively based on the prime number a, the prime number b, and the Jacobian addition candidate value j,

a security judging procedure for searching for a candidate value h meeting a security condition such as almost prime number characteristic from the class H , according to the class H , and

a parameter deciding procedure for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a , the prime number b , and the prime number p , respectively based on the prime number a , the prime number b , the prime number p , and the candidate value h .

Other objects, features and advantages of the present invention will become clear from the detailed description given herebelow.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood more fully from the detailed description given herebelow and from the accompanying drawings of the preferred embodiment of the invention, which, however, should not be taken to be limitative to the invention, but are for explanation and understanding only.

In the drawings:

Fig. 1 is a block diagram showing the form of the first embodiment according to the present invention;

5 Fig. 2 is a flow chart showing the operation of a Stickelberger element computing device;

Fig. 3 is a flow chart showing an operation of the Jacobian additive candidate value computing device;

Fig. 4 is a flow chart showing the operation of the order candidate value computing device;

10 Fig. 5 is a flow chart showing the parameter deciding device;

Fig. 6 is a block diagram showing the form of the third embodiment of the present invention.

15 DESCRIPTION OF THE PREFERRED EMBODIMENT

The preferred embodiment of the present invention will be discussed hereinafter in detail with reference to the accompanying drawings. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be obvious, however, to those skilled in the art that the present invention may be practiced without these specific details. In other instance, well-known structures are not shown in detail in order to 20 unnecessary obscure the present invention.

25 First, the principle of the present invention will be described.

The present invention is to efficiently search for an algebraic curve such that the order of the Jacobian group is almost a prime number, from the class of an algebraic curve having the definition expression such as $\alpha Y^a + \beta X^b + 1 = 0$, and to make it possible to use a higher and complicated algebraic curve that couldn't be used, for an algebraic curve cryptography. Here, the parameters a and b indicate the degree of complexity of curves.

The algebraic curve over a finite field F_q of the order q, which has the definition expression such as $\alpha Y^a + \beta X^b + 1 = 0$, is defined as $C(q, \alpha, \beta)$. As for the algebraic curve $C(q, \alpha, \beta)$, the order of the Jacobian group can be designed using the description about its L function by use of the Jacobian addition.

Hereafter, for brief description, assume that $q := p$ (p is expressed by q) is a prime number, and that the expression, $p \equiv 1 \pmod{\text{LCM}(a, b)}$ is satisfied (LCM is the least common multiple). Further, the primitive ab root of 1 is defined as ζ . The prime number p is completely factorized into m pieces of prime ideals, P_1, P_2, \dots, P_m in a cyclotomic $Q(\zeta)$. Here, the number m is the number of irreducible residue classes of the divisor ab.

The generator w of the multiplication group F_p^* of the finite field F_p is fixed, and the index χ_s of F_p^* , as for the rational number such that $(p-1)s$ becomes an

integer, is defined as $\chi_s(w) = \exp(2\pi i s)$ (where i is an imaginary number). Assuming that $\chi_s(0) = 0$ (s : when it is not an integer), $=1$ (s : when it is an integer), the domain is expanded on the whole F_p . As for the integer $l=1, 2, \dots, a-1$ and the integer $m=1, 2, \dots, b-1$, the expression, $j_p(l, m) = \sum_{\{1+v_1+v_2=0\}} \chi_{1/a}(v_1) \chi_{m/b}(v_2)$ is called as Jacobian addition. Where, v_1 and v_2 run on $v_1, v_2 \in F_p$ meeting the equation $1+v_1+v_2=0$. At this time, it is well known that the L function $L_p(U)$ of $C(p, \alpha, \beta)$ can be expressed by using the Jacobian addition as follows.

$L_p(U) = \prod_{l=1, 2, \dots, a-1, m=1, 2, \dots, b-1} (1 + \chi_{1/a}(\alpha^{-1}) \chi_{m/b}(\beta^{-1}) j_p(l, m) U)$. Therefore, the order h of the Jacobian group of $C(p, \alpha, \beta)$ is given by $h = L_p(1) = \prod_{l=1, 2, \dots, a-1, m=1, 2, \dots, b-1} (1 + \chi_{1/a}(\alpha^{-1}) \chi_{m/b}(\beta^{-1}) j_p(l, m))$. It is necessary to calculate the Jacobian addition $j_p(l, m)$, in order to require the order of the Jacobian group. However, since it is impossible to directly calculate the Jacobian addition $j_p(l, m)$ according to the definition expression, from the viewpoint of the volume of calculation, the Stickelberger element as for the following Jacobian addition is used.

Assume that $[\lambda]$ indicates the maximum integer not exceeding the rational number λ and that $\langle \lambda \rangle$ indicates the fraction part $\lambda - [\lambda]$ of the rational number λ . Further, assume that σ_t indicates the Galois mapping

$\zeta \rightarrow \zeta^t$ of the cyclotomic field $Q(\zeta)$. The Stickelberger element $\omega(a, b)$ that is the generator of the group ring $Z[Gal(Q(\zeta) | Q)]$ is defined as $\omega(a, b) = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_t^{-1}$. Where, t runs on the typical series of the 5 irreducible residue class with the divisor ab .

It is well known that the expression $(j_p(l, m)) = P^{\omega(a, b)}$ is satisfied as the ideal of the cyclotomic field $Q(\zeta)$. Where, P is the prime ideal on p . By the above expression, $j_p(l, m)$ is necessarily resolved except for the 10 $2ab$ root of 1. Of the results, the degree of freedom for ab root can be obtained by the degree of freedom of the coefficient $\alpha, \beta \in F_q$ of $C(p, \alpha, \beta)$.

In these ways, the search algorithm of the following secure curve $C(p, \alpha, \beta)$ can be obtained.

15 The search algorithm of the secure curve $C(p, \alpha, \beta)$ input: the number of Jacobian bits n

output: p, α, β

(1) $g \leftarrow (a-1)(b-1)/2$

20 (2) The candidate j of the Jacobian addition as for the prime number p of some n/g bit or the like is searched for by using the calculation algorithm of the candidate value of the Jacobian addition as described later:

(p, j) \leftarrow {calculation algorithm of the candidate value of the Jacobian addition}(n/g).

25 (3) as for the respective $k = 0, 1, \dots, ab$,

$h_k \leftarrow \prod_{i=1, 2, \dots, a-1, m=1, 2, \dots, b-1} (1 + (-\zeta)^k j)$

(4) Check whether there is an almost prime number h_k in

{ h_0, h_1, \dots, h_{ab} }. If there is none, return to (1). If there is, $h := h_k$ is defined.

(5) The symbols ζ_a, ζ_b are respectively defined as a-root of 1 and b-root of 1 in F_p . Check whether the order 5 of the Jacobian group of the curve $C(p, \zeta_a^{-1}, \zeta_b^m): \zeta_a^{-1} y^a + \zeta_b^m x^b + 1 = 0$ is equal to h , as for the respective $l = 0, 1, \dots, a-1$ and the respective $m = 0, 1, \dots, b-1$. If it is equal, output $p, \alpha = \zeta_a^{-1}, \beta = \zeta_b^m$ and finish the operation. If such l and m don't exist, return to (2).

10 In the calculation algorithm of the candidate value of the Jacobian addition used in the above, the candidate value of the Jacobian addition is required by using the above-mentioned Stickelberger element $\omega(a, b) = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t}^{-1}$.

15 The calculation algorithm of the candidate value of the Jacobian addition is as follows.

input: the number of bits m ,

output: p, j ,

(1) $\omega \leftarrow \sum_t (\langle t/a \rangle + \langle t/b \rangle) \sigma_{-t}^{-1}$,

20 (2) Generate $\gamma_0 = \sum_{i=0}^{m-1} c_i \zeta^i$ ($-10 < c_i < 10$) at random.

(3) as for the respective $i = 1, 2, \dots$,

$\gamma \leftarrow \gamma_0 + I$,

$p \leftarrow \text{Norm}_{\Omega(\zeta)/\Omega}(\gamma)$,

Is p smaller than m bit or so?

25 yes \rightarrow continue,

Is p larger than m bit or so?

yes \rightarrow to (2),

Is p a prime number?

no → continue,

(4) Output $j \leftarrow \gamma^\omega$, p and j, and finish.

This time, the form of the first embodiment of
5 the present invention will be described with reference
to the accompanying drawings. Fig. 1 is a block diagram
showing the form of the first embodiment.

With reference to Fig. 1, the form of the first
embodiment of the present invention comprises a
10 Stickelberger element computing device 11, a Jacobian
addition candidate value computing device 12, an order
candidate value computing device 13, a security judging
device 14, a parameter deciding device 15, a memory 16,
an input device 17, an output device 18, and a central
15 processing unit 19.

The memory 16 includes a a-storing file 161, a
b-storing file 162, a ω -storing file 163, a j-storing
file 164, an H-storing file 165, an h-storing file 166,
a p-storing file 167, and an n-storing file 168.

20 Hereinafter, assume that a known method is used
for the norm arithmetic $N_{Q(\zeta)/Q}$ and four fundamental
arithmetic rules of algebraic number in the cyclotomic
field $Q(\zeta)$, arithmetic of the function of the Galois
group $G(Q(\zeta)/Q)$ for the cyclotomic field $Q(\zeta)$, and
25 addition and multiplication in the group ring $Z[G(Q(\zeta)/Q)]$
on the Galois group $G(Q(\zeta)/Q)$ of the integer ring Z
coefficient.

The operation of the form of a first embodiment according to the present invention will be described this time.

Fig. 2 is a flow chart showing the operation of the Stickelberger element computing device 11. Fig. 3 is a flow chart showing the operation of the Jacobian addition candidate value computing device 12. Fig. 4 is a flow chart showing the operation of the order candidate value computing device 13. Fig. 5 is a flow chart showing the operation of the parameter deciding device 15.

The description will be made in the case where two different prime numbers, $a=3$, $b=7$, specifying the degree of complexity of a curve, and the size $n=160$ of an encryption key to be used are supplied from the input device 17. The supplied a and b are temporarily stored in the a -storing file 161 and the b -storing file 162 respectively, through the central processing unit 19. Further, a variable found in the following description is stored in the memory 16.

The Stickelberger element computing device 11 obtains $a=3$, $b=7$ from the a -storing file 161 and the b -storing file 162, according to the operation as shown in Fig. 2, and operates as follows.

A typical series $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ of the irreducible residue class with $a \cdot b = 3 \times 7 = 21$ used for the variable L as the divisor is stored

in Step S21 of Fig. 2.

As for the respective integers t included in the variable $L=\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

in Step 22 of Fig. 2, for example, as for $t=1$, since

5 $[<1/3>+<1/7>] = [1/3+1/7]=[10/21]=0$, 0 is stored in the variable m ; since $-1^{-1} \equiv -1 \equiv 20 \pmod{21}$, 20 is stored in the variable s ; since $0 \times \sigma_{20} = 0$, 0 is stored in the variable λ_1 .

As for the other t , since

10 $[<2/3>+<2/7>]=[2/3+2/7]=[20/21]=0$, 0 is stored in the variable λ_2 ; since $[<4/3>+<4/7>]=[1/3+4/7]=[19/21]=0$, 0 is stored in the variable λ_4 ; since

$[<5/3>+<5/7>]=[2/3+5/7]=[29/21]=1$ and $(-5)^{-1} \equiv 16^{-1} \equiv 4 \pmod{21}$, σ_4 is stored in the variable λ_5 ; since

15 $[<8/3>+<8/7>]=[2/3+1/7]=[17/21]=0$, 0 is stored in the variable λ_8 ; since $[<10/3>+<10/7>]=[1/3+3/7]=[16/21]=0$, 0 is stored in the variable λ_{10} ; since

$[<11/3>+<11/7>]=[2/3+4/7]=[26/21]=1$ and $(-11)^{-1} \equiv 10^{-1} \equiv 19 \pmod{21}$, σ_{19} is stored in the variable λ_{11} ; since

20 $[<13/3>+<13/7>]=[1/3+6/7]=[25/21]=1$ and $(-13)^{-1} \equiv 8^{-1} \equiv 8 \pmod{21}$, σ_8 is stored in the variable λ_{13} ; since

$[<16/3>+<16/7>]=[1/3+2/7]=[13/21]=0$, 0 is stored in the variable λ_{16} ; since $[<17/3>+<17/7>]=[2/3+3/7]=[23/21]=1$

and $(-17)^{-1} \equiv 4^{-1} \equiv 16 \pmod{21}$, σ_{16} is stored in the

variable λ_{17} ; since $[<19/3>+<19/7>]=[1/3+5/7]=[22/21]=1$

and $(-19)^{-1} \equiv 2^{-1} \equiv 11 \pmod{21}$, σ_{11} is stored in the

variable λ_{19} ; and since

[$<20/3>+<20/7>$]=[$2/3+6/7$]=[$32/21$]=1 and $(-20)^{-1} \equiv 1^{-1} \equiv 1 \pmod{21}$, σ_1 is stored in the variable λ_{20} , in the same way.

5 The total $\omega = \sigma_4 + \sigma_{19} + \sigma_8 + \sigma_{16} + \sigma_{11} + \sigma_1$ of
the whole data stored in the respective variables $\lambda_1, \lambda_2,$
 $\lambda_4, \lambda_5, \lambda_8, \lambda_{10}, \lambda_{11}, \lambda_{13}, \lambda_{16}, \lambda_{17}, \lambda_{19}, \lambda_{20}$ is computed
in Step S23 of Fig. 2. Here, the total means the total
in the group ring $\mathbb{Z} [G(\mathbb{Q}(\zeta) \mid \mathbb{Q})]$, indicating the total
of the coefficients of the respective σ_i with the
10 respective σ_i regarded as symbols. The arithmetic result
 ω is temporarily stored in the ω -storing file 163
through the central processing unit 19.

15 The Jacobian addition candidate value computing
device 12 obtains $a=3, b=7, n=160, \omega=\sigma_4 + \sigma_{19} + \sigma_8 + \sigma_{16}$
 $+ \sigma_{11} + \sigma_1$ from the a -storing file 161, the b -storing
file 162, the n -storing file 168, and the ω -storing file
163 and computes the candidate value j of the Jacobian
addition, according to the processing as shown in Fig. 3,
as follows.

20 Since $ab=21$, the primitive 21st power root of 1
is stored in the variable ζ , and since $2n / (a-1)(b-1) =$
 $26.6\dots, 27$ is stored in the variable m , in Step 31 of
Fig. 3.

25 The random integer of the cyclotomic field $\mathbb{Q}(\zeta)$
is stored in the variable γ_0 as follow, in Step S32 of
Fig. 3. The variable γ_0 is initialized to 0; the random
number $r_0 = -2$ is generated as for $t=0$, $r_0 \zeta^0 = -2$ is

added to γ_0 , so to require $\gamma_0 = -2$; the random number $r_1 = 2$ is generated as for $t=1$, $r_1 \zeta^1 = 2 \zeta$ is added to γ_0 , so to require $\gamma_0 = -2 + 2\zeta$; and the same operation is repeated until $t=11$, so to require $\gamma_0 = -2 + 2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$, in Step S32 of Fig. 3.

The following operation will be performed on the respective integers $i=0, 1, 2, \dots$, in Step S33 of Fig.

3. As for $i=0$, $\gamma_0 + 0$ is stored in the variable γ , so to obtain $\gamma = -2 + 2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$, to compute the norm $N_{Q(\zeta)|_Q}(\gamma)$. The resultant 129571513 is stored in the p-storing file 167, the number of bits 29 of $p = 129571513$ is stored in the variable 1. That $l=29$ and $m=27$ or so is confirmed. When $p = 129571513$ is factorized into prime factors in the known way, $p = 129571513 = 43 \times 211 \times 14281$ is obtained. Since $p = 129571513$ is not a prime number, the operation as for $i = 0$ is finished, and as for $i = 1$, the same operation will be repeated. In the form of this embodiment, the same operation is continued until $i = 2$. As for $i = 2$, $\gamma_0 + 2$ is stored in the variable γ , so to obtain $\gamma = 2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$, to compute the norm $N_{Q(\zeta)|_Q}(\gamma)$. The resultant 163255597 is stored in the p-storing file 167, and the number of bits 28 of $p = 163255597$ is stored in the variable 1. Since $l=28$ and $m=27$ or so, and $p = 163255597$ is determined as a prime number (a known method is used

for judgment of a prime number), the operation of Step S33 will be finished.

In Step S34 of Fig. 3, the Stickelberger element $\omega = \sigma_4 + \sigma_{19} + \sigma_8 + \sigma_{16} + \sigma_{11} + \sigma_1$ is adopted to work on the value $2\zeta - \zeta^2 + 2\zeta^3 + 2\zeta^5 - \zeta^6 - \zeta^7 - 2\zeta^8 + 2\zeta^9 - \zeta^{11}$ of the variable γ and the result is stored in the j-storing file 164.

Namely, since $j = \sigma_4(\gamma) \sigma_{19}(\gamma) \sigma_8(\gamma) \sigma_{16}(\gamma) \sigma_{11}(\gamma) \sigma_1(\gamma) = -11346 + 4158\zeta + 9337\zeta^2 - 10930\zeta^3 + 3060\zeta^4 + 11132\zeta^5 - 1408\zeta^6 - 10000\zeta^7 + 7506\zeta^8 + 1237\zeta^9 - 9894\zeta^{10} + 16406\zeta^{11}$, the content of the j-storing file 164 becomes $-11346 + 4158\zeta + 9337\zeta^2 - 10930\zeta^3 + 3060\zeta^4 + 11132\zeta^5 - 1408\zeta^6 - 10000\zeta^7 + 7506\zeta^8 + 1237\zeta^9 - 9894\zeta^{10} + 16406\zeta^{11}$.

The order candidate value computing device 13 obtains a, b, j respectively from the a-storing file 161, the b-storing file 162, and the j-storing file 164, according to the processing as shown in Fig. 4, and computes each candidate value for the order of the Jacobian group, as follows.

Since $ab=21$, the primitive 21st power root of 1 is stored in the variable ζ , in Step S41 of Fig. 4.

In Step S42 of Fig. 4, $N_{\Omega(\zeta)}|_{\Omega} (1 + (-\zeta)^k j)$ is computed as for the respective integers $k=1, \dots, 2ab=42$, by using the Jacobian addition candidate value j, and the result is stored in the variable h_k . Namely, since $N_{\Omega(\zeta)}|_{\Omega} (1 + (-\zeta)^k j)$

=18945750554224674862720917379214050968749547249577 as
for k=1,
18945750554224674862720917379214050968749547249577 is
stored in the variable h_1 , and since $N_{0(\zeta)}|_0 (1 + (-\zeta)^2 j)$
5 = 18928969305265796978830941938772180777050417721949 as
for k=2,
18928969305265796978830941938772180777050417721949 is
stored in the variable h_2 .

10 Hereinafter, in the same way,
18939442397757559639176586128404383479076142135761 is
stored in the variable h_3 ;
18935060345406437247984249590121980321244862496761 is
stored in the variable h_4 ;
15 18935622676852726684902816970612470237474541809664 is
stored in the variable h_5 ;
18931936903665705475581647305574444786263237069081 is
stored in the variable h_6 ;
18929560654771860101383318185997674116929626012889 is
20 stored in the variable h_7 ;
18939150203650250186166315242126355786799280592469 is
stored in the variable h_8 ;
18932675807273674693936115572103379669380378369473 is
stored in the variable h_9 ;
25 18942309965821405414970614992239749691042375170033 is
stored in the variable h_{10} ;
18934229290635176830764035532046510839791719442389 is

DRAFT - DO NOT DISTRIBUTE

stored in the variable h_{11} ;
18935834172588603026508807514961653603431968293369 is
stored in the variable h_{12} ;
18938078743053945947831932134835899678969080710281 is
5 stored in the variable h_{13} ;
18930980854114698521197692341107826796840225368461 is
stored in the variable h_{14} ;
18925926348482126046797408190951930473609373791353 is
stored in the variable h_{15} ;
10 18936229724314338327608155999193464492913218459633 is
stored in the variable h_{16} ;
18935389098278487495205740285052812170943878823253 is
stored in the variable h_{17} ;
18931691567781542998050896522571358027374445665073 is
15 stored in the variable h_{18} ;
18932734180610926108166703609049207716180145717849 is
stored in the variable h_{19} ;
18938664411743724815803784593761801461579705647693 is
stored in the variable h_{20} ;
20 18933942752770105179837989473472080616474423254969 is
stored in the variable h_{21} ;
18919302986335777367049540268484273861903106390769 is
stored in the variable h_{22} ;
18936075396885270373781711765180522497408613713621 is
25 stored in the variable h_{23} ;
18925604328984592629627465194343191206594160037073 is
stored in the variable h_{24} ;

18929984863788418751836156261712299372083231633577 is
stored in the variable h_{25} ;

18929422531793648170111228339741198150094983499776 is
stored in the variable h_{26} ;

5 18933107954541528865152848804062672753166448460761 is
stored in the variable h_{27} ;

18935483634705487053043563594391048299333735703993 is
stored in the variable h_{28} ;

18925896848340062851972136696783348221127455098349 is
stored in the variable h_{29} ;

10 18932368490475205159124453933007681555744686326777 is
stored in the variable h_{30} ;

18922739336864448742750281538719599103232717642873 is
stored in the variable h_{31} ;

15 18930815175217344826609492375186423724694014551957 is
stored in the variable h_{32} ;

18929210510360406226057659372472230885175421077009 is
stored in the variable h_{33} ;

18926967327936730178250537884862137815188718140673 is
20 stored in the variable h_{34} ;

18934063763272126450623787600233843527396400812437 is
stored in the variable h_{35} ;

18939120559761876801054292506881700885415287701041 is
stored in the variable h_{36} ;

25 18928816315710623530089460607608797337081800632473 is
stored in the variable h_{37} ;

18929656538570982720438072809652072203857571941789 is

stored in the variable h_{38} ;
18933352933862176606331230531189579186007983024249 is
stored in the variable h_{39} ;
18932310663274994445599743180032079937147687805121 is
5 stored in the variable h_{40} ;
18926381945702726406182624557022344113037957991709 is
stored in the variable h_{41} ; and
18931102681789095072229676262975577344314266433617 is
stored in the variable h_{42} , respectively.

10

Finally, the order candidate value computing device 13 combines the contents of the variables h_1 to h_{42} together as H and stores the same into the H -storing file 165.

15

The security judging device 14 obtains the H from the H -storing file 165, and searches for a candidate value h meeting the security condition of almost prime number characteristic from the order candidate values h_1, h_2, \dots, h_{42} included in the H , and
20 stores the same into the h -storing file 166. In this form of the embodiment, for brief description, the security condition is considered as for the almost prime number characteristic. By use of the known prime number judging method, $h_{11} =$

25

18934229290635176830764035532046510839791719442389 is judged to be a prime number, and the security judging device 14 stores $h = h_{11} =$

DOCUMENT EDITION

18934229290635176830764035532046510839791719442389 into
the h-storing file 166.

The parameter deciding device 15 obtains a, b, p,
and h respectively from the a-storing file 161, the b-
5 storing file 162, the p-storing file 167, and the h-
storing file 166, and operates according to the
processing as shown in Fig. 5.

In Step S51 of Fig. 5, 127994587 that is the
primitive 3rd power root of 1 with p = 163255597 used as
10 the divisor is stored in the variable ζ_3 , and 8342648
that is the primitive 7th power root of 1 with p =
163255597 used as the divisor is stored in the variable
 ζ_7 .

15 In Step S52 of Fig. 5, the following processing
will be performed on the respective integers l=1, 2, 3
and the respective integers m=1, 2, 3, 4, 5, 6, 7.

When l=1 and m=1, $\zeta_3 = 127994587$ is stored in
20 the variable ε , and $\zeta_7 = 8342648$ is stored in the
variable η . The random element {151707017 + 104678491 x
+ 123646083 x² + 18753988 y + 87634493 x³ + 61274336 x y
+ x⁴, 138799785 + 145105684 x + 584395 x² + 80828873 y +
34715892 x³ + 121885874 x y + 59787844 x⁴ + x² y,
25 161162224 + 117150097 x + 100956100 x² + 89380061 y +
140032555 x³ + 43367019 x y + y²} of the Jacobian group
of an algebraic curve defined by the expression $\varepsilon y^3 + \eta$

$x^7 + 1 = 127994587$ $y^3 + 8342648 x^7 + 1 = 0$ is generated,
and this is stored in the variable G, the power of
h=18934229290635176830764035532046510839791719442389 in
the Jacobian group, on a point stored in the variable G
5 is computed, and the result {133659497 + 103424746 x +
136032897 $x^2 + 131029199 y + 24618867 x^3 + 114944034 x y$
+ $x^4, 86125426 + 125891893 x + 19568269 x^2 + 27044314 y +$
80420960 $x^3 + 137562092 x y + x^2 y, 53604112 + 65990501 x$
+ 51269221 $x^2 + 55271502 y + 7974233 x^3 + 84922220 x y +$
10 $y^2 }$ is stored in the variable G.

Since the above content of the variable G is not
equal to the identity element {} in the Jacobian group, ζ
 $_{_3} = 127994587$ is stored in the variable ε , and $\zeta_{_7}^2 =$
 $8342648^2 \bmod 163255597 = 159772073$ is stored in the
15 variable η , as for l = 1 and m = 2, thereby repeating
the above processing.

In the case of the form of this embodiment, when
l = 2 and m=2, $\varepsilon = 35261009$ and $\eta = 159772073$ are
obtained, the power of
20 h=18934229290635176830764035532046510839791719442389 on
the point G = {4568071 + 141843715 x + 68256743 $x^2 +$
71903501 y + 128953783 $x^3 + 10781960 x y + x^4, 48272788 +$
45615229 x + 150692034 $x^2 + 53973350 y + 11114765 x^3 +$
78550130 x y + 61331354 $x^4 + x^2 y, 117552807 + 135448907$
25 x + 64074711 $x^2 + 141058974 y + 49208246 x^3 + 93940317 x$
 $y + y^2 }$ generated at random results in the identity
element {}, and the parameter deciding device 15

supplies $p=163255597$, $\varepsilon=35261009$, $\eta=159772073$ as the parameters of a secure algebraic curve.

Finally, the parameters $p=163255597$, $\varepsilon=35261009$, $\eta=159772073$ supplied by the parameter deciding device 15 5 are supplied from the output device 18.

This time, the form of a second embodiment according to the present invention will be described in detail.

The form of the second embodiment according to the present invention is a secure parameter generating method in an algebraic curve cryptography, comprising:

(a) a Stickelberger element computing procedure of requiring the prime numbers a and b respectively from the a -storing file 161 and the b -storing file 162 and computing the Stickelberger element ω in the ab portion of the cyclotomic field;

(b) a procedure of storing the Stickelberger element ω computed in the above Stickelberger element computing procedure into the ω -storing file 163;

(c) a Jacobian addition candidate value computing procedure of requiring the prime number a , the prime number b , the size n of an encryption key, and the Stickelberger element ω respectively from the a -storing file 161, the b -storing file 162, the n -storing file 168, and ω -storing file 163 and computing the Jacobian addition candidate value j as for the two different prime numbers a and b and the prime number p

corresponding to the Jacobian addition candidate value
j;

(d) a procedure of storing the prime number p and the
Jacobian addition candidate value j computed in the
above Jacobian addition candidate value computing
procedure, respectively into the p-storing file 167 and
the j-storing file 164;

(e) an order candidate value computing procedure of
requiring the prime number a, the prime number b, and
the Jacobian candidate value j respectively from the a-
storing file 161, the b-storing file 162, and the j-
storing file 164 and computing the class H consisting of
a plurality of candidate values for the order of the
Jacobian group of the algebraic curve specified by the
prime number a and the prime number b;

(f) a procedure of storing the class H computed in the
above order candidate value computing procedure into the
H-storing file 165;

(g) a security judging procedure of requiring the class
H from the H-storing file 165 and searching for the
candidate value h meeting the security condition such as
almost prime number characteristic;

(h) a procedure of storing the candidate value h found
in the above security judging procedure, into the h-
storing file 166; and

(i) a parameter deciding procedure of requiring the
prime number a, the prime number b, the prime number p,

DRAFT EDITION 0

and the candidate value h respectively from the a-storing file 161, the b-storing file 162, the p-storing file 167, and the h-storing file 166 and computing a parameter of an algebraic curve whose order of the

5 Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a , the prime number b , and the prime number p .

The form of a third embodiment according to the present invention will be described in detail with reference to the drawings, this time. Fig. 6 is a block diagram showing the form of the third embodiment according to the present invention.

With reference to Fig. 6, the form of the third embodiment of the present invention is a storing medium 130 for storing a program for running the respective procedures according to the form of the second embodiment of the present invention, on a computer 100. This program is executed after being loaded in a storage of the computer 100.

The present invention is effective in enabling the use of a higher and complicated algebraic curve which couldn't be used, for an algebraic curve cryptography, and improving the security of the algebraic curve cryptography. This is because an algebraic curve having a prime number substantially as the order of the Jacobian group can be found efficiently from the class of algebraic curves having the following

DRAFTED IN JAPANESE

definition equation; $\alpha Y^a + \beta X^b + 1 = 0$, thereby expanding the range of the usable algebraic curves and dispersedly increasing the decoding work of a hacker.

Although the invention has been illustrated and
5 described with respect to exemplary embodiment thereof,
it should be understood by those skilled in the art that
the foregoing and various other changes, omissions and
additions may be made therein and thereto, without
departing from the spirit and scope of the present
10 invention. Therefore, the present invention should not
be understood as limited to the specific embodiment set
out above but to include all possible embodiments which
can be embodies within a scope encompassed and
equivalents thereof with respect to the feature set out
15 in the appended claims.

WHAT IS CLAIMED IS:

1. A secure parameter generating device in an algebraic curve cryptography, comprising:

an input means for receiving two different prime numbers (a, b) specifying degree of complexity of a curve and size (n) of an encryption key to be used;

5 a Stickelberger element computing device for computing a Stickelberger element (ω) in an ab cyclotomic, based on the prime number (a) and the prime number (b);

10 a Jacobian addition candidate value computing device for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b, and a prime number p corresponding to the Jacobian addition candidate value j , based on the prime number (a), the prime number (b), the size (n) of an encryption key, and the Stickelberger element (ω) ;

15 an order candidate value computing device for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b, based on the prime number a, the prime number b, and the Jacobian addition candidate value j ;

20 a security judging device for searching for a candidate value h meeting a security condition such as almost prime number characteristic from the class H ,

SEARCHED SERIALIZED INDEXED

according to the class H;

a parameter deciding device for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a, the prime number b, and the prime number p, based on the prime number a, the prime number b, the prime number p, and the candidate value h; and

an output device for supplying the parameter of the algebraic curve computed by said parameter deciding device.

2. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

an a-storing means, a b-storing means, and an n-storing means for respectively storing the prime number a, the prime number b, and the size n of the encryption key received by said input means;

a ω -storing means for storing a Stickelberger element ω computed by said Stickelberger element computing device;

a p-storing means and a j-storing means for respectively storing the prime number p and the Jacobian addition candidate value j computed by said Jacobian addition candidate value computing device;

15 an H-storing means for storing the class H

computed by said order candidate value computing device;
and

an h-storing means for storing the candidate
value h found by said security judging device.

20

3. A secure parameter generating device in an
algebraic curve cryptography as claimed in Claim 1,
further comprising:

5 said Stickelberger element computing device for
computing the Stickelberger element ω by use of the
equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs
on a typical series of irreducible residue class with ab
used as a divisor, $[\lambda]$ indicates the maximum integer not
exceeding a rational number λ , $\langle \lambda \rangle$ indicates a
10 fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t
indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic
(ζ is the primitive ab root of 1)), based on the prime
number a and the prime number b.

4. A secure parameter generating device in an
algebraic curve cryptography as claimed in Claim 1,
further comprising:

5 said Jacobian addition candidate value computing
device for generating α at random, which is an algebraic
integer γ generating a prime ideal of a cyclotomic K
generated by the primitive ab root of 1 and whose
absolute norm becomes the prime number p of bit length

2010 RELEASE UNDER E.O. 14176

10 $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$.

5. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b ; and

15 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the

Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$.

6. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the 10 class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

7. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_t \{-t^{-1}\}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a 10 fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t

indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

15 said order candidate value computing device for
computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab
cyclotomic K), as for each k that is an integer from 1
20 to $2ab$ inclusively, when ζ is the primitive ab root of 1,
based on the prime number a , the prime number b , and the
Jacobian addition candidate value j , and computing the
class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

8. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$; and

15 said order candidate value computing device for
computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab
cyclotomic K), as for each k that is an integer from 1
20 to $2ab$ inclusively, when ζ is the primitive ab root of 1,
based on the prime number a , the prime number b , and the
Jacobian addition candidate value j , and computing the
class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

9. A secure parameter generating device in an
algebraic curve cryptography as claimed in Claim 1,
further comprising:

5 said Stickelberger element computing device for
computing the Stickelberger element ω by use of the
equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs
on a typical series of irreducible residue class with ab
used as a divisor, $[\lambda]$ indicates the maximum integer not
exceeding a rational number λ , $\langle \lambda \rangle$ indicates a
10 fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t
indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic
(ζ is the primitive ab root of 1)), based on the prime
number a and the prime number b ;

15 said Jacobian addition candidate value computing
device for generating α at random, which is an algebraic
integer γ generating a prime ideal of a cyclotomic K

generated by the primitive ab root of 1 and whose
absolute norm becomes the prime number p of bit length
2n/(a-1)(b-1) or so, based on the prime number a, the
20 prime number b, the size n of the encryption key,
and the Stickelberger element ω , and computing the
Jacobian addition candidate value j by use of the
equation $j = \gamma^\omega$; and

25 said order candidate value computing device for
computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab
cyclotomic K), as for each k that is an integer from 1
30 to 2ab inclusively, when ζ is the primitive ab root of 1,
based on the prime number a, the prime number b, and the
Jacobian addition candidate value j, and computing the
class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

10. A secure parameter generating device in an
algebraic curve cryptography as claimed in Claim 1,
further comprising:

5 said parameter deciding device for requiring the
primitive a root ζ_a and the primitive b root ζ_b of 1
with the prime number p used as the divisor, based on
the prime number a, the prime number b, the prime number
p, and the candidate value h, generating a random point
G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a$

10 $+ \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^1 , and ζ_b^m as the parameter of an algebraic curve whose order of
15 the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

11. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

10 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number

20 p , and the candidate value h , generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} Y^a + \zeta_b^{-m} X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^{-1} , and ζ_b^{-m} as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

12. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$; and

10 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1

with the prime number p used as the divisor, based on the prime number a , the prime number b , the prime number p , and the candidate value h , generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

13. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the 10 class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$; and

15 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of 25 the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

14. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a 10 fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic

DRAFT EDITION 0

(ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

15 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$; and

25 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} Y^a + \zeta_b^{-m} X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^{-m} as the parameter of an algebraic curve whose order of 35 the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

DRAFT - 2023-08-28

15. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b ;

10 said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$; and

15 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on

the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} Y^a + \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

16. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

5 said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$;

10 said order candidate value computing device for

15 computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$; and

20 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a , the prime number b , the prime number p , and the candidate value h , generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^{-m} x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^{-1} , and ζ_b^{-m} as the parameter of an algebraic curve whose order of

25 the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

30

35

17. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1,

further comprising:

5 said Stickelberger element computing device for
computing the Stickelberger element ω by use of the
equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs
on a typical series of irreducible residue class with ab
used as a divisor, $[\lambda]$ indicates the maximum integer not
exceeding a rational number λ , $\langle \lambda \rangle$ indicates a
10 fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t
indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic
(ζ is the primitive ab root of 1)), based on the prime
number a and the prime number b ;

15 said Jacobian addition candidate value computing
device for generating α at random, which is an algebraic
integer γ generating a prime ideal of a cyclotomic K
generated by the primitive ab root of 1 and whose
absolute norm becomes the prime number p of bit length
2n/(a-1)(b-1) or so, based on the prime number a , the
20 prime number b , the size n of the encryption key,
and the Stickelberger element ω , and computing the
Jacobian addition candidate value j by use of the
equation $j = \gamma^\omega$;

25 said order candidate value computing device for
computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab
cyclotomic K), as for each k that is an integer from 1

30 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H=\{h_1, h_2, \dots, h_{2ab}\}$; and

35 said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a , the prime number b , the prime number p , and the candidate value h , generating a random point G over an algebraic curve defined by the equation $\zeta_a^l y^a + \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^l , and ζ_b^m as the parameter of an algebraic curve whose order of 40 the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an 45 identity element in the Jacobian group.

18. A secure parameter generating method in an algebraic curve, comprising the steps of:

5 a Stickelberger element computing procedure for computing a Stickelberger element ω in an ab cyclotomic, respectively based on two different prime numbers a and b specifying degree of complexity of curve;

a Jacobian addition candidate value computing

procedure for computing Jacobian addition candidate
value j corresponding to the two different prime numbers
10 a and b, and a prime number p corresponding to the
Jacobian addition candidate value j, respectively based
on the prime number a, the prime number b, the size n of
an encryption key, and the Stickelberger element ω ;

an order candidate value computing procedure for
15 computing a class H consisting of a plurality of
candidate values for order of a Jacobian group of an
algebraic curve specified by the prime number a and the
prime number b, respectively based on the prime number a,
the prime number b, and the Jacobian addition candidate
20 value j;

a security judging procedure for searching for a
candidate value h meeting a security condition such as
almost prime number characteristic from the class H,
according to the class H; and

25 a parameter deciding procedure for computing a
parameter of an algebraic curve whose order of the
Jacobian group is in accord with the candidate value h,
of the algebraic curves specified by the prime number a,
the prime number b, and the prime number p, respectively
30 based on the prime number a, the prime number b, the
prime number p, and the candidate value h.

19. A secure parameter generating method in an
algebraic curve cryptography as claimed in Claim 18,

further comprising:

5 a procedure for storing a Stickelberger element
ω computed by said Stickelberger element computing
procedure into said ω-storing means;

10 a procedure for respectively storing the prime
number p and the Jacobian addition candidate value j
computed by said Jacobian addition candidate value
computing procedure into said p-storing means and j-
storing means;

15 a procedure for storing the class H computed by
said order candidate value computing procedure into said
H-storing means; and

20 a procedure for storing the candidate value h
found by said security judging procedure into said h-
storing means.

20. A secure parameter generating method in an
algebraic curve cryptography as claimed in Claim 18,
further comprising:

5 said Stickelberger element computing procedure
for computing the Stickelberger element ω by use of the
equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs
on a typical series of irreducible residue class with ab
used as a divisor, $[\lambda]$ indicates the maximum integer not
exceeding a rational number λ , $\langle \lambda \rangle$ indicates a
10 fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t
indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic

(ζ is the primitive ab root of 1)), based on the prime number a and the prime number b.

21. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

5 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a, 10 the prime number b, the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$.

22. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

5 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a 10 fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t

RECORDED
SEARCHED
INDEXED
SERIALIZED
FILED

indicates Galois mapping $\zeta \rightarrow \zeta^e$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

15 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$.

20 23. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

25 said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

DRAFT - DRAFT - DRAFT - DRAFT -

24. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

5 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b ; and

10
15 said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2 ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the 20 class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

25. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18,

PCT/US2016/033256

further comprising:

5 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a ,
10 the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$; and

15 said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a , the prime number b , and the Jacobian addition candidate value j , and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$.

26. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

5 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the

equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t-1\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

10 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$; and

15 said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \text{Norm}_{K/Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K/Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to $2ab$ inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the

class of the candidate values, $H=\{h_1, h_2, \dots, h_{2ab}\}$.

27. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

5 said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} Y^a + \zeta_b^{-m} X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^{-m} as the parameter of an algebraic curve whose order of 15 the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

28. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

5 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs

on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle\lambda\rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

10 said parameter deciding procedure for requiring
15 the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m as the parameter of an algebraic curve whose order of
20 25 the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

29. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

29.1. said Jacobian addition candidate value computing

5 procedure for generating α at random, which is an
algebraic integer γ generating a prime ideal of a
cyclotomic K generated by the primitive ab root of 1 and
whose absolute norm becomes the prime number p of bit
length $2n/(a-1)(b-1)$ or so, based on the prime number a ,
10 the prime number b , the size n of the encryption key,
and the Stickelberger element ω , and computing the
Jacobian addition candidate value j by use of the
equation $j = \gamma^\omega$; and

15 said parameter deciding procedure for requiring
the primitive a root ζ_a and the primitive b root ζ_b of 1
with the prime number p used as the divisor, based on
the prime number a , the prime number b , the prime number
 p , and the candidate value h , generating a random point
20 G over an algebraic curve defined by the equation $\zeta_a^{-l} Y^a$
+ $\zeta_b^{-m} X_b + 1 = 0$, as for each integer l from 1 to a
inclusively and each integer m from 1 to b inclusively,
computing the h -fold of an element in the Jacobian group
indicated by the point G , and supplying p , ζ_a^{-l} , and ζ_b^{-m}
25 as the parameter of an algebraic curve whose order of
the Jacobian group is in accord with the candidate value
 h , of the algebraic curves specified by the prime number
 a and the prime number b if the result is equal to an
identity element in the Jacobian group.

30. A secure parameter generating method in an
algebraic curve cryptography as claimed in Claim 18,

further comprising:

5 said order candidate value computing procedure
for computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-$
 $\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab
cyclotomic K), as for each k that is an integer from 1
10 to $2ab$ inclusively, when ζ is the primitive ab root of 1,
based on the prime number a, the prime number b, and the
Jacobian addition candidate value j, and computing the
class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$; and

15 said parameter deciding procedure for requiring
the primitive a root ζ_a and the primitive b root ζ_b of 1
with the prime number p used as the divisor, based on
the prime number a, the prime number b, the prime number
p, and the candidate value h, generating a random point
G over an algebraic curve defined by the equation $\zeta_a^{-1} Y^a$
20 $+ \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a
inclusively and each integer m from 1 to b inclusively,
computing the h-fold of an element in the Jacobian group
indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m
as the parameter of an algebraic curve whose order of
25 the Jacobian group is in accord with the candidate value
h, of the algebraic curves specified by the prime number
a and the prime number b if the result is equal to an
identity element in the Jacobian group.

31. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

5 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{\{-t^{-1}\}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b ;

10 15 20 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length $2n/(a-1)(b-1)$ or so, based on the prime number a , the prime number b , the size n of the encryption key, and the Stickelberger element ω , and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^\omega$; and

25 said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a , the prime number b , the prime number

30 p, and the candidate value h, generating a random point
G over an algebraic curve defined by the equation $\zeta_a^{-1} Y^a$
+ $\zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a
inclusively and each integer m from 1 to b inclusively,
computing the h-fold of an element in the Jacobian group
indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m
as the parameter of an algebraic curve whose order of
35 the Jacobian group is in accord with the candidate value
h, of the algebraic curves specified by the prime number
a and the prime number b if the result is equal to an
identity element in the Jacobian group.

32. A secure parameter generating method in an
algebraic curve cryptography as claimed in Claim 18,
further comprising:

5 said Stickelberger element computing procedure
for computing the Stickelberger element ω by use of the
equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_{-t^{-1}}$ (where, t runs
on a typical series of irreducible residue class with ab
used as a divisor, $[\lambda]$ indicates the maximum integer not
exceeding a rational number λ , $\langle \lambda \rangle$ indicates a
10 fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t
indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic
(ζ is the primitive ab root of 1)), based on the prime
number a and the prime number b;

15 said order candidate value computing procedure
for computing a candidate value h_k for the order of the

Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \text{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$; and

20 said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a + \zeta_b^{-m} x^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^{-m} as the parameter of an algebraic curve whose order of

25 the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

30

35

33. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

5 said Jacobian addition candidate value computing
procedure for generating α at random, which is an
algebraic integer γ generating a prime ideal of a
cyclotomic K generated by the primitive ab root of 1 and
whose absolute norm becomes the prime number p of bit
length $2n/(a-1)(b-1)$ or so, based on the prime number a ,
10 the prime number b , the size n of the encryption key,
and the Stickelberger element ω , and computing the
Jacobian addition candidate value j by use of the
equation $j = \gamma^\omega$;

15 said order candidate value computing procedure
for computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-$
 $\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab
cyclotomic K), as for each k that is an integer from 1
20 to $2ab$ inclusively, when ζ is the primitive ab root of 1,
based on the prime number a , the prime number b , and the
Jacobian addition candidate value j , and computing the
class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$; and

25 said parameter deciding procedure for requiring
the primitive a root ζ_a and the primitive b root ζ_b of 1
with the prime number p used as the divisor, based on
the prime number a , the prime number b , the prime number
 p , and the candidate value h , generating a random point
30 G over an algebraic curve defined by the equation $\zeta_a^{-1} Y^a$
 $+ \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a

inclusively and each integer m from 1 to b inclusively, computing the h -fold of an element in the Jacobian group indicated by the point G , and supplying p , ζ_a^1 , and ζ_b^m as the parameter of an algebraic curve whose order of 35 the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

34. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

5 said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_t^{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ , $\langle \lambda \rangle$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b ;

10 said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit

length $2n/(a-1)(b-1)$ or so, based on the prime number a ,
20 the prime number b , the size n of the encryption key,
and the Stickelberger element ω , and computing the
Jacobian addition candidate value j by use of the
equation $j = \gamma^\omega$;

25 said order candidate value computing procedure
for computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-$
 $\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab
cyclotomic K), as for each k that is an integer from 1
30 to $2ab$ inclusively, when ζ is the primitive ab root of 1,
based on the prime number a , the prime number b , and the
Jacobian addition candidate value j , and computing the
class of the candidate values, $H = \{h_1, h_2, \dots, h_{2ab}\}$; and

35 said parameter deciding procedure for requiring
the primitive a root ζ_a and the primitive b root ζ_b of 1
with the prime number p used as the divisor, based on
the prime number a , the prime number b , the prime number
 p , and the candidate value h , generating a random point
40 G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a$
 $+ \zeta_b^{-m} x^b + 1 = 0$, as for each integer l from 1 to a
inclusively and each integer m from 1 to b inclusively,
computing the h -fold of an element in the Jacobian group
indicated by the point G , and supplying p , ζ_a^{-1} , and ζ_b^{-m}
as the parameter of an algebraic curve whose order of
45 the Jacobian group is in accord with the candidate value

h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

35. A computer readable memory storing a program for generating a secure parameter in an algebraic curve cryptography, to run the program on a computer, the program comprising the steps of:

5 a Stickelberger element computing procedure for computing a Stickelberger element ω in an ab cyclotomic, respectively based on two different prime numbers a and b specifying degree of complexity of curve;

10 a Jacobian addition candidate value computing procedure for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b, and a prime number p corresponding to the Jacobian addition candidate value j, respectively based on the prime number a, the prime number b, the size n of 15 an encryption key, and the Stickelberger element ω ;

20 an order candidate value computing procedure for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b, respectively based on the prime number a, the prime number b, and the Jacobian addition candidate value j;

a security judging procedure for searching for a

candidate value h meeting a security condition such as
25 almost prime number characteristic from the class H ,
according to the class H ; and

a parameter deciding procedure for computing a
parameter of an algebraic curve whose order of the
Jacobian group is in accord with the candidate value h ,
30 of the algebraic curves specified by the prime number a ,
the prime number b , and the prime number p , respectively
based on the prime number a , the prime number b , the
prime number p , and the candidate value h .

~~36.~~ A computer readable memory storing a program for
generating a secure parameter in an algebraic curve
cryptography,

the program comprising the steps of:

5 said Stickelberger element computing procedure
for computing the Stickelberger element ω by use of the
equation $\omega = \sum_t [\langle t/a \rangle + \langle t/b \rangle] \sigma_t^{-\{t^{-1}\}}$ (where, t runs
on a typical series of irreducible residue class with ab
used as a divisor, $[\lambda]$ indicates the maximum integer not
10 exceeding a rational number λ , $\langle \lambda \rangle$ indicates a
fractional portion $\lambda - [\lambda]$ of the rational number λ , σ_t
indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic
(ζ is the primitive ab root of 1)), based on the prime
number a and the prime number b .

15 ~~37.~~ A computer readable memory storing a program for

generating a secure parameter in an algebraic curve
cryptography,

the program comprising the steps of:

5 said Jacobian addition candidate value computing
procedure for generating α at random, which is an
algebraic integer γ generating a prime ideal of a
cyclotomic K generated by the primitive ab root of 1 and
whose absolute norm becomes the prime number p of bit
10 length $2n/(a-1)(b-1)$ or so, based on the prime number a ,
the prime number b , the size n of the encryption key,
and the Stickelberger element ω , and computing the
Jacobian addition candidate value j by use of the
equation $j = \gamma^\omega$.

15 38. A computer readable memory storing a program for
generating a secure parameter in an algebraic curve
cryptography,

the program comprising the steps of:

5 said order candidate value computing procedure
for computing a candidate value h_k for the order of the
Jacobian group of an algebraic curve specified by the
parameters a and b , using the equation $h_k = \text{Norm}_{K|Q}(1 + (-$
 $\zeta)^k j)$ (where $\text{Norm}_{K|Q}$ is a norm mapping in the ab
10 cyclotomic K), as for each k that is an integer from 1
to $2ab$ inclusively, when ζ is the primitive ab root of 1,
based on the prime number a , the prime number b , and the
Jacobian addition candidate value j , and computing the

class of the candidate values, $H=\{h_1, h_2, \dots, h_{2ab}\}$.

15

39. A computer readable memory storing a program for
generating a secure parameter in an algebraic curve
cryptography,

the program comprising the steps of:

5

said parameter deciding procedure for requiring
the primitive a root ζ_a and the primitive b root ζ_b of 1
with the prime number p used as the divisor, based on
the prime number a, the prime number b, the prime number
p, and the candidate value h, generating a random point
10 G over an algebraic curve defined by the equation $\zeta_a^{-1} y^a$
 $+ \zeta_b^m x^b + 1 = 0$, as for each integer l from 1 to a
inclusively and each integer m from 1 to b inclusively,
computing the h-fold of an element in the Jacobian group
indicated by the point G, and supplying p, ζ_a^{-1} , and ζ_b^m
15 as the parameter of an algebraic curve whose order of
the Jacobian group is in accord with the candidate value
h, of the algebraic curves specified by the prime number
a and the prime number b if the result is equal to an
identity element in the Jacobian group.

RECORDED - INDEXED - SERIALIZED - FILED

ABSTRACT OF THE DISCLOSURE

The Stickelberger element computing device
computes a Stickelberger element ω in an ab cyclotomic;
the Jacobian addition candidate value computing device
5 computes the Jacobian addition candidate value j and a
prime number p corresponding to the Jacobian addition
candidate value j, based on the prime number a, the
prime number b, the size n of an encryption key, and the
Stickelberger element ω ; the order candidate value
10 computing device computes a class H consisting of a
plurality of candidate values for the order of the
Jacobian group of an algebraic curve, based on the prime
number a, the prime number b, and the Jacobian addition
candidate value j; the security judging device searches
15 for a candidate value h meeting a security condition
such as almost prime number characteristic from the
class H; and the parameter deciding device computes a
parameter of an algebraic curve whose order of the
Jacobian group is in accord with the candidate value h,
20 of the algebraic curves specified by the prime number a,
the prime number b, and the prime number p.

DISCLOSURE REFERENCES

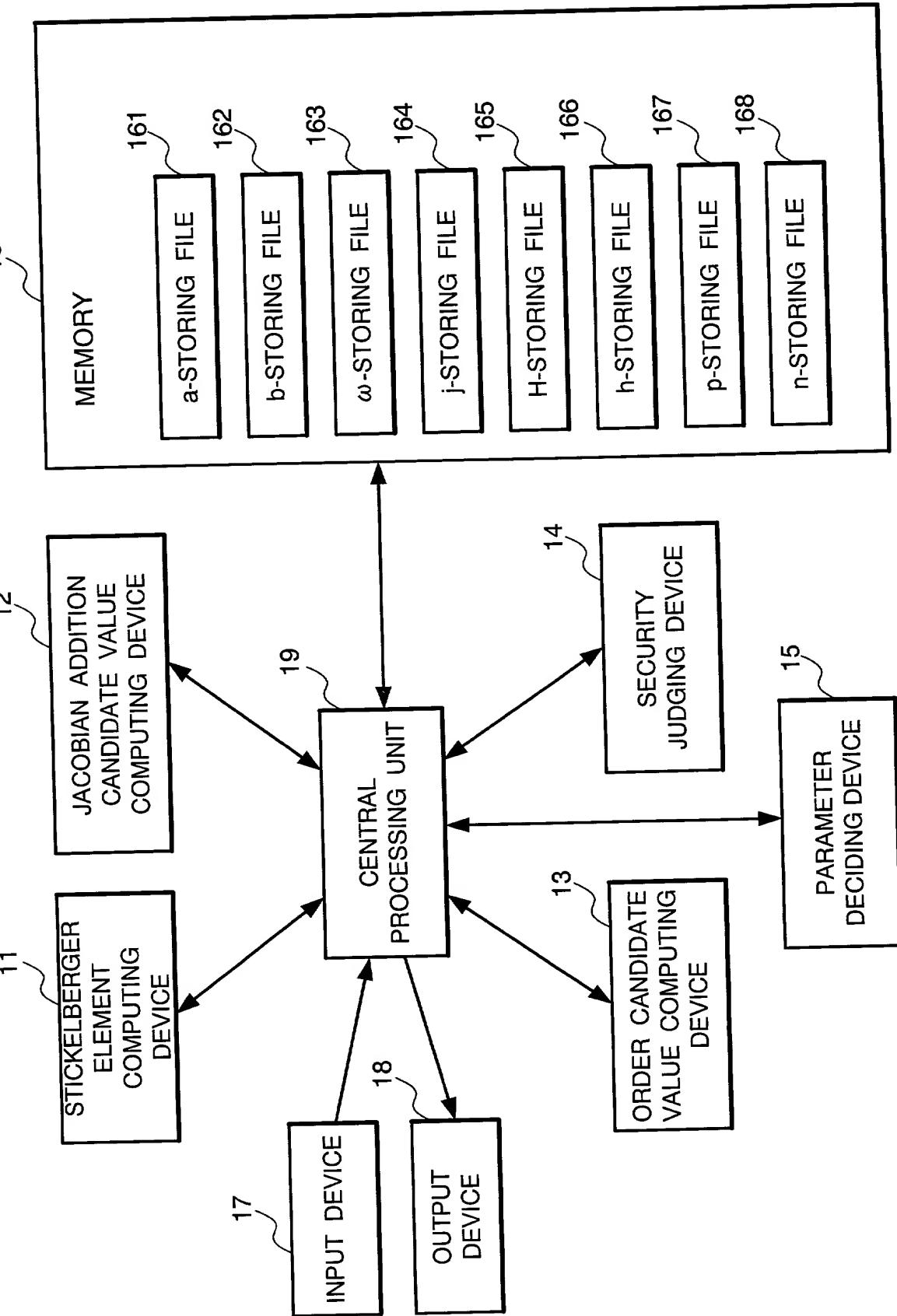
FIG. 1

FIG. 2

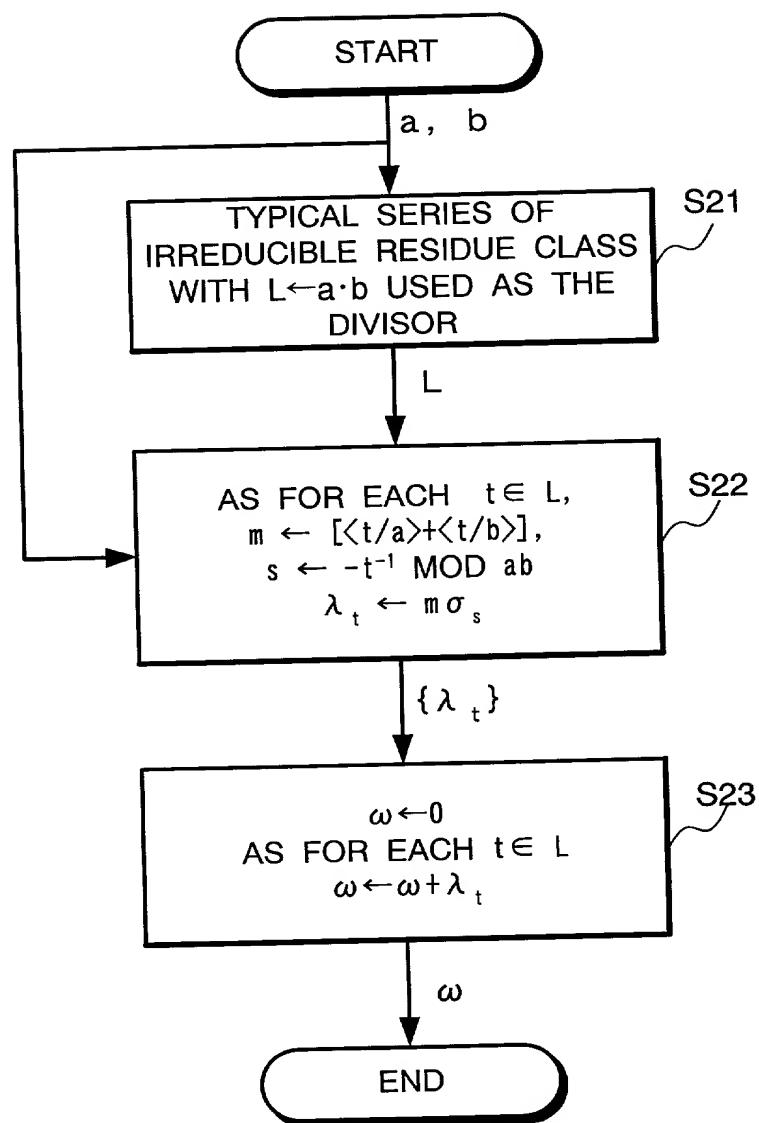


FIG. 3

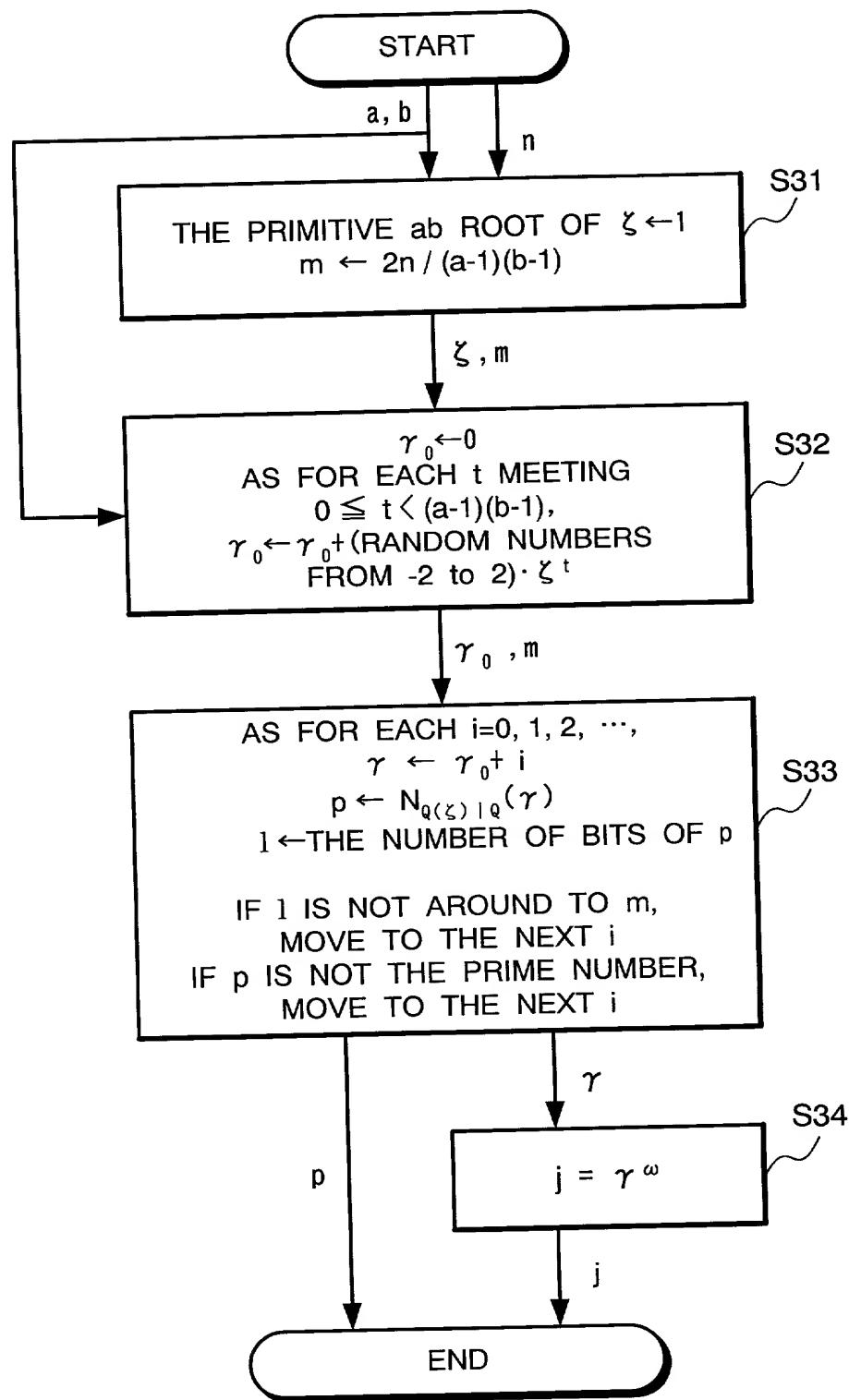


FIG. 4

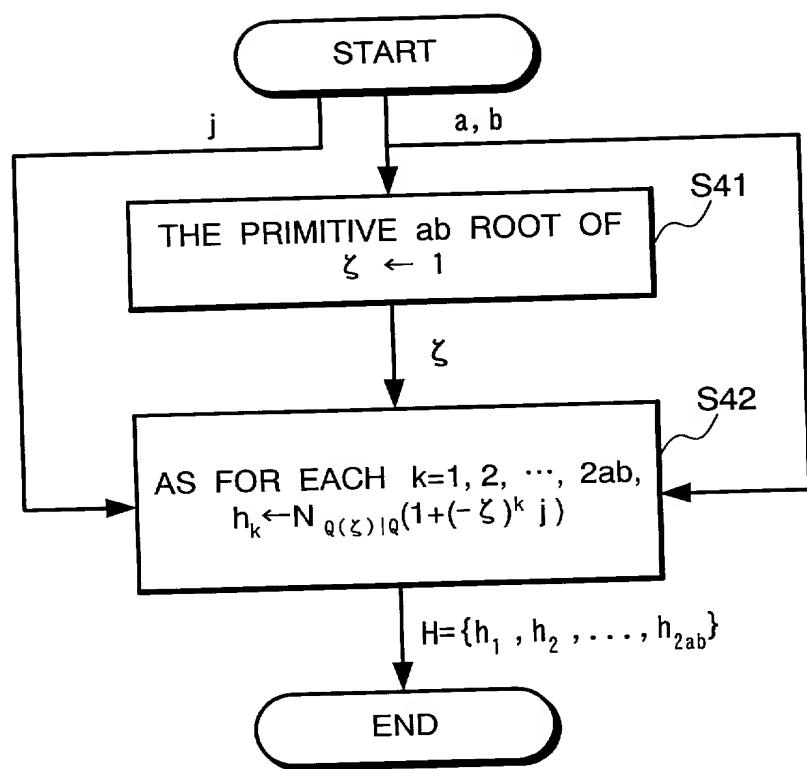


FIG. 5

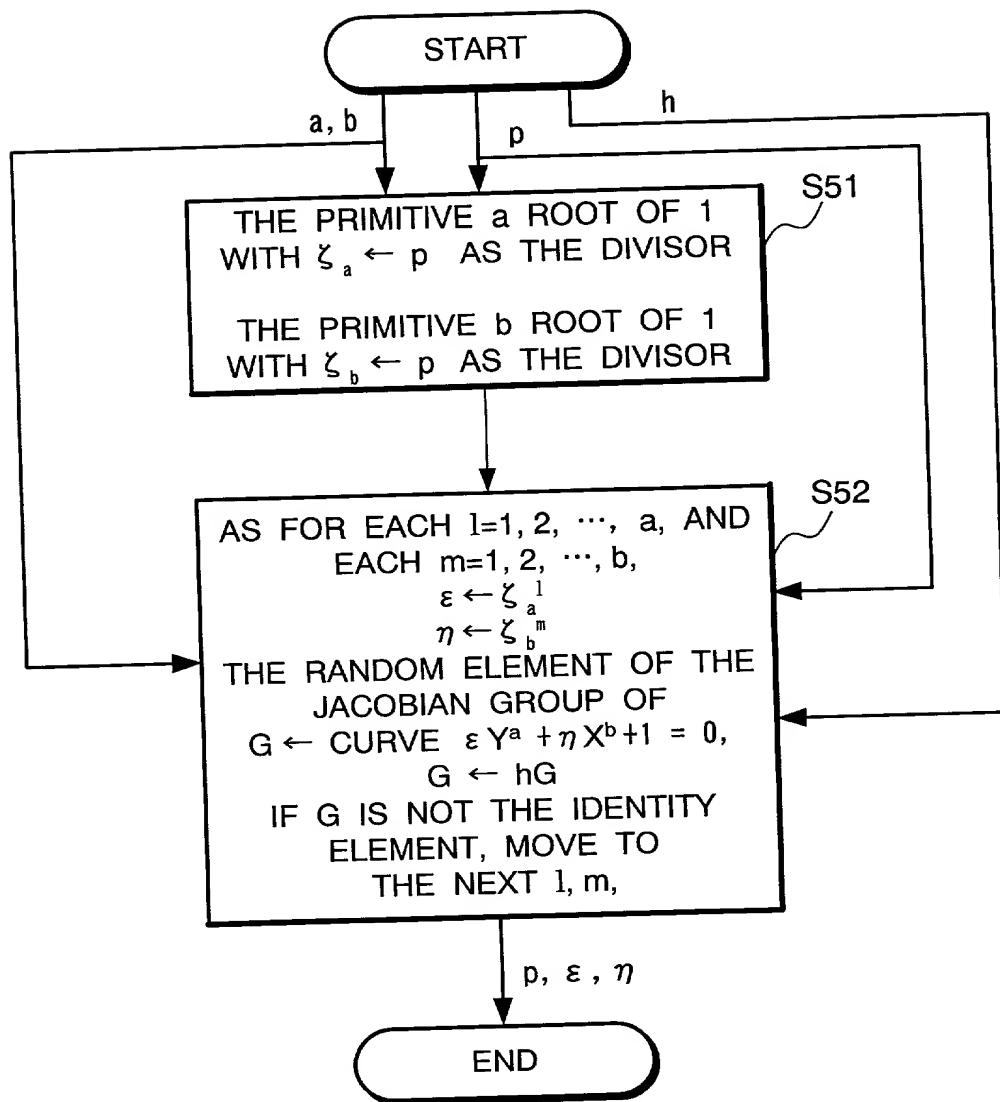
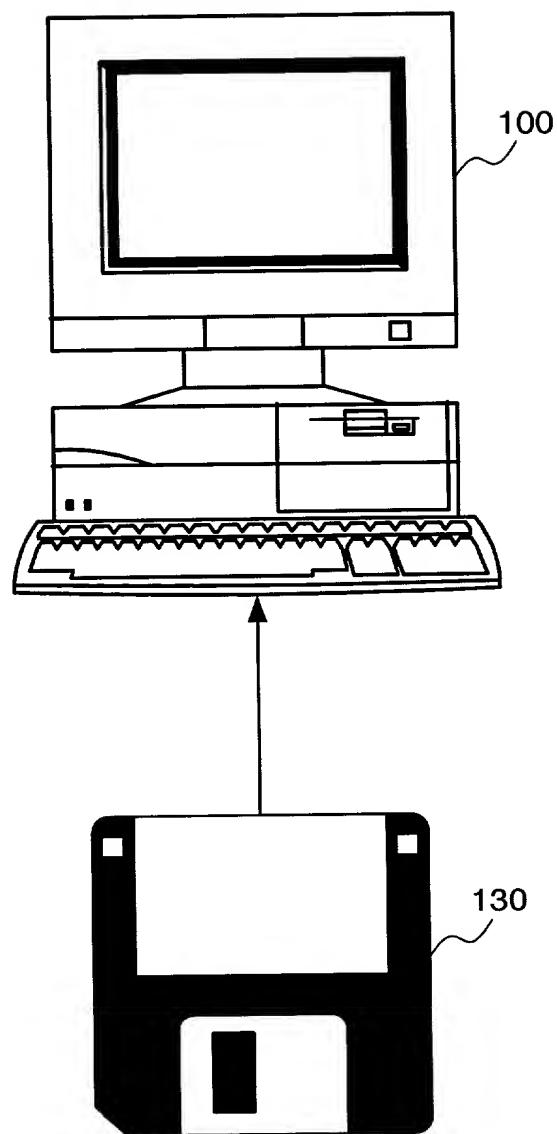


FIG. 6

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SECURE PARAMETER GENERATING DEVICE AND PARAMETER GENERATING METHOD IN
the specification of which is attached hereto unless the following box is checked: ALGEBRAIC CURVE CRYPTOGRAPHY

was filed on _____ as United States Application Number or PCT International Application Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is known by me to be material to patentability as defined in Title 37, Code of Federal Regulations § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

NUMBER	COUNTRY	DAY/MONTH/YEAR FILED	PRIORITY CLAIMED
11-242075	Japan	27/August/1999	Yes

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

APPLICATION NO.	FILING DATE

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is known by me to be material to patentability as defined in Title 37, Code of Federal Regulations § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

APPLICATION SERIAL NO.	FILING DATE	STATUS: PATENTED, PENDING, ABANDONED

I hereby appoint as my attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Stephen A. Bent, Reg. No. 29,768; David A. Blumenthal, Reg. No. 26,257; John J. Feldhaus, Reg. No. 28,822; Donald D. Jeffery, Reg. No. 19,980; Eugene M. Lee, Reg. No. 32,039; Peter G. Mack, Reg. No. 26,001; Brian J. McNamara, Reg. No. 32,789; Sybil Meloy, Reg. No. 22,749; George E. Quillin, Reg. No. 32,792; Colin G. Sandercock, Reg. No. 31,298; Bernhard D. Saxe, Reg. No. 28,665; Charles F. Schill, Reg. No. 27,590; Richard L. Schwaab, Reg. No. 25,479; Arthur Schwartz, Reg. No. 22,115; Harold C. Wegner, Reg. No. 25,258.

Address all correspondence to FOLEY & LARDNER, Washington Harbour, 3000 K Street, N.W., Suite 500, P.O. Box 25696, Washington, D.C. 20007-8696. Address telephone communications to David A. Blumenthal at (202) 672-5300.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of First or Sole Inventor Seigo ARITA	Signature of First or Sole Inventor <i>Seigo Arita</i> 	Date Aug.14,2000
Residence Address Tokyo, Japan	Country of Citizenship Japan	
Post Office Address c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan		

Full Name of Second Inventor	Signature of Second Inventor	Date
Residence Address	Country of Citizenship	
Post Office Address		

Full Name of Third Inventor	Signature of Third Inventor	Date
Residence Address	Country of Citizenship	
Post Office Address		

Full Name of Fourth Inventor	Signature of Fourth Inventor	Date
Residence Address	Country of Citizenship	
Post Office Address		

Full Name of Fifth Inventor	Signature of Fifth Inventor	Date
Residence Address	Country of Citizenship	
Post Office Address		